Q1 Team Name

0 Points

INSYNC

Q2 Commands

10 Points

List all the commands in sequence used from the start screen of this level to the end of the level. (Use -> to separate the commands)

```
4->enter->jump->jump->back->pull->back->back->enter->wave->back->back->thrnxxtzy->read->134721542097659029845273957->c->read->password
```

Q3 CryptoSystem

5 Points

What cryptosystem was used at this level? Please be precise.

6 Round DES(Block Cipher)

Q4 Analysis

80 Points

Knowing which cryptosystem has been used at this level, give a detailed description of the cryptanalysis used to figure out the password. (Use Latex wherever required. If your solution is not readable, you will lose marks. If necessary, the file upload option in this question must be used TO SHARE IMAGES ONLY.)

Initially we needed to collect the wand from the river. Then we went back and freed the spirit in level 3. After coming back to the first screen of level 4, we typed ‘read’, read the instructions provided and typed ‘password’ as was instructed in the message. We then got the ciphertext - ‘nghnffiqrskpkgmkgfkspsrknneojrhk’. We had to decrypt this ciphertext to cross level 4.
Now it was written on the previous screen that it is using 6 round DES(and surely not using 10-round DES). We tried solving the assignment using 4-round DES but it didn't work. So, it was also not 4 round DES. Based on hint provided in the game we tried using 6-round DES. One instruction provided in the game which we noticed was "two letters for one byte". DES has block size of 8 bytes hence we will have 16 letters in one block.After doing a deep analysis of plain-text and cipher-text pairs we noticed that cipher-text consists of only 16 letters in the interval [d-s] which was confirmed as we can represent 16 characters using 4 bits. So, our plaintext/ciphertext space was from 'd' to 's'. For further processing, we carried out the mapping of [d-s] to [0-15].
#1 To break it, we used Differential Crypt-Analysis with chosen-plaintext attack to carry out the process and decided to use two 3-round characteristic in-order to break 6-round DES. The differential iterative characteristic used was:
$C1 => 40080000\ 04000000$ and
$C2 => 00200008\ 00000400$
both with probabilities $1/16$.
#2 Now, we applied inverse initial permutations to both the characteristics and got:
$InvPerm(C1) => 00\ 00\ 80\ 10\ 00\ 00\ 40\ 00$
$InvPerm(C2) => 00\ 00\ 08\ 01\ 00\ 10\ 00\ 00$
So, now we generated 1000 plaintext pairs such that their XOR was InvPerm(C1) and another 1000 pairs such that the XOR is InvPerm(C2) and stored them in plaintext1.txt and plaintext2.txt.
#3 After this, we created a python script to pass all these pairs to the game and collect the ciphertexts corresponding to them. We stored the corresponding responses in ciphertexts1.txt and ciphertexts2.txt.

- i]: We used the mapping of characters defined above to convert the obtained ciphertext to binary and then, we used DesAnalysis.py to apply reverse final permutation on these binary

ciphertexts to get $(L_6 R_6)$ and $(L_6' R_6')$, which is output of the 6^{th} round of DES. We know that, $R_5 = L_6$,
therefore using the values R_5 and R_5', we computed output of Expansion box and input XOR of S-boxes for 6^{th} round.
- ii] : For the first characteristic mentioned above, $L_5 = 04000000$ and for the second characteristic $L_5 = 00000400$. We found output of permutation box by performing $L_5 \oplus (R_6 \oplus R_6')$, then we applied inverse permutation on this value to obtain output XOR of S-boxes for 6^{th} round.
- iii]: Let $E(R_5) = \alpha_1 \alpha_2 \cdots \alpha_8$ and $E(R_5') = \alpha_1' \alpha_2' \cdots \alpha_8'$ and $\beta_i = \alpha_i \oplus k_{6,i}$ and $\beta_i' = \alpha_i' \oplus k_{6,i}$, where $|\alpha_i| = 6 = |\alpha_i'|$ and $k_6 = k_{6,1} k_{6,2} \cdots k_{6,8}$. At this point, we know $\alpha_i, \alpha_i', \beta_i \oplus \beta_i'$ and $\gamma_i \oplus \gamma_i'$. We created a $8 * 64$ key matrix to store the number of times a key $k \in [1, 64]$ satisfies the possibility of being a key to S_i box, where $i \in [1, 8]$.

- iv]: We computed the set $X_i = (\beta, \beta') \mid \beta \oplus \beta' = \beta_i \oplus \beta_i'$ and $S(\beta) \oplus S(\beta') = \gamma_i \oplus \gamma_i'$. Then, we found the key k, such that $\alpha_i \oplus k = \beta$ and $(\beta, \beta') \in X_i$ for some β'. For all the keys k which satisfied this condition for S_i box, we incremented their count in the key matrix i.e. key_matrix[i][k] was incremented.
- After performing the above analysis to find the keys, we obtained the following results for characteristic 4008000004000000 :

S-box	Max	Mean	Key
S1	146	68	45
S2	330	79	51
S3	121	70	37
S4	105	65	7
S5	157	70	62
S6	329	76	24
S7	182	71	19
S8	187	69	36

For this characteristic, in round $4, XOR$ will be zero for $S2, S5, S6$, S7 and S8. Therefore, in round 6 these S-boxes will give the corresponding key bits of K_6. Also, it can be observed that a significant difference is seen in the maximum key frequency and mean key frequency for these S-boxes which further assures of these key values being correct. We proceeded by taking the key bits for $\mathrm{S2},\ \mathrm{S5},\ \mathrm{S6},\ \mathrm{S7}$ and $\mathrm{S8}$ boxes as $51, 7, 24, 19$ and 36 respectively.

For characteristic 0020000800000400 we got the following result for the S-boxes:

S-box	Max	Mean	Key
S1	173	70	45
S2	151	70	51
S3	127	65	37
S4	307	84	7
S5	173	68	62
S6	290	78	24
S7	116	62	19
S8	105	67	36

For this characteristic, in round 4 , XOR will be zero for $\mathrm{S1},\ \mathrm{S2},\ \mathrm{S4}$, S5 and S6. Therefore, in round 6 these S-boxes will give the corresponding key bits of K_6. Also, it can be observed that a significant difference is seen in the maximum key frequency and mean key frequency for these S-boxes. We proceeded by taking the key bits for $\mathrm{S1},\ \mathrm{S2},\ \mathrm{S4},\ \mathrm{S5}$ and $\mathrm{S6}$ boxes as $45, 51, 7, 62$ and 24 respectively.

Now, S2,S5 and S6 are common in both the Characteristics.
So now, we took key values for $\mathrm{S1},\ \mathrm{S2},\ \mathrm{S4},\ \mathrm{S5}$, S6, S7 and S8 as 45, 51, 7, 62, 24, 19 and 36 for round key K_6. So, now we have 42 bits of the 56 bit key.

We used the key scheduling algorithm and got the following partial master key:

$$\mathbf{X11XX1XX01011X100XX11X11000X1010111X00}$$

Here X is for unknown bits.
- Now, we have 14 unknown bits and for these 14 unknown bits of DES key, we iterate through all 2^{14} possible permutations of the key to find the correct key. Using plaintext as "ddddddd

dddddddd" and the corresponding ciphertext as "ofjopjgi iodmmrkj", we tried 6 round DES encryption.The key which gave the correct cipher is the final key. After running our code, we got the correct key as:

0110111001011110011110110000101011110000100

We also found the 48 bit round key for all the 6-rounds using this key, which were as follows:

Round 1 11101100010011110000011100001111011

Round 2 01101111001101110110001000100100011

Round 3 11101010110101001110110111111111000

Round 4 11011001110000110101101010000111110

Round 5 00100100110110111011101100010101101

Round 6 10110111001110010100011111111001100

The above process was done by using DesAnalysis.py

The ciphertext that we had got after reaching the game screen was "nghnffiqrskpkgmkgfkspsrknneojrhk". The ascii mapping for this was [163, 74, 34, 93, 239, 124, 115, 151, 50, 127, 207, 231, 170, 27, 110, 71].Since, each character is represented by 4 bits, so this is 128 bit string or 2 blocks of DES Cipher.

We decrypted this ciphertext using decrypt.cpp and got the plaintext as:

nrtqhwijie000000

After removing the padded 0's, we finally got:

Password: nrtqhwijie

This was our password which we used to clear the level.

References:

https://medium.com/lotus-fruit/breaking-des-using-differential-

cryptanalysis-958e8118ff41
https://en.wikipedia.org/wiki/Differential_cryptanalysis

No files uploaded

Q5 Password

5 Points

What was the password used to clear this level?

nrtqhwijie

Q6 Codes

0 Points

Unlike previous assignments, this time it is MANDATORY that you upload the codes used in the cryptanalysis. If you fail to do so, you will be given 0 marks for the entire assignment.

▾ Team_INSYNC.zip Download

```
Large file hidden. You can download it using the button above.
```

Assignment 4

● GRADED

GROUP

Punit Chaudhari
Piyush Gangle
Aman Mittal
View or edit group

TOTAL POINTS

72.5 / 100 pts

QUESTION 1 Team Name	**0** / 0 pts
QUESTION 2 Commands	**10** / 10 pts
QUESTION 3 CryptoSystem	**5** / 5 pts
QUESTION 4 Analysis	**80** / 80 pts
QUESTION 5 Password	**5** / 5 pts
QUESTION 6 Codes	**-27.5** / 0 pts